**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/60

A1

(11) International Publication Number: **WO 99/66436**

(43) International Publication Date: 23 December 1999 (23.12.99)

(21) International Application Number: PCT/GB99/01886

(22) International Filing Date: 18 June 1999 (18.06.99)

(30) Priority Data:
60/089,825 19 June 1998 (19.06.98) US

(71) Applicant: PROTX LIMITED [GB/GB]; 38 Belgrave Square, London SW1X 8NT (GB).

(72) Inventors: SLATER, Candida, Coralie, Anne; 15 Marlborough Street, London SW3 3PS (GB). DOWNS, Iain; 18 Gladsmuir Road, London N19 8JE (GB).

(74) Agent: LUCKHURST, Anthony, Henry, William; Marks & Clerk, 57–60 Lincoln's Inn Fields, London WC2A 3LS (GB).

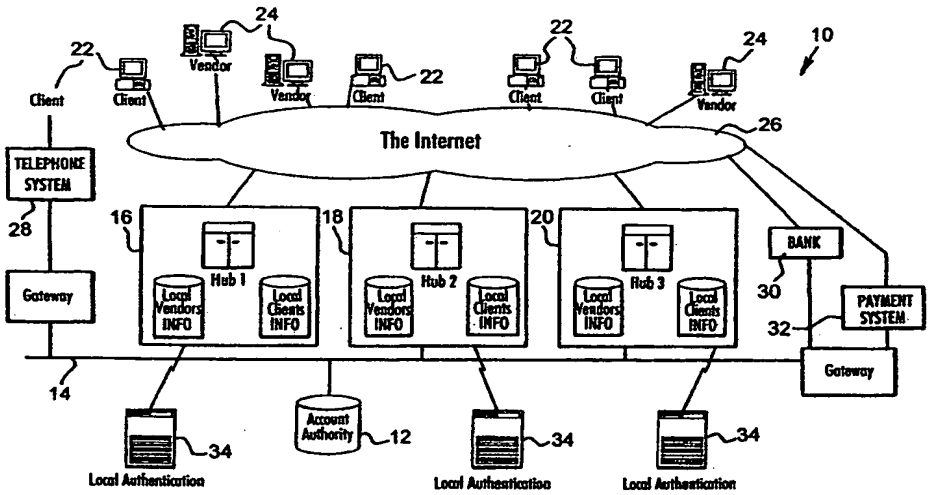
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*

(54) Title: VERIFIED PAYMENT SYSTEM

(57) Abstract

A distributed verified trusted third–party system (VPS) (10) and method enable electronic/digital transactions through real–time verification and authentication, with improved privacy and security, encompassing the whole payment range from very large to very small. The VPS (10) includes hubs (16–20) storing client data and connecting clients (22) to vendors (24) to mediate secure electronic transactions. Date may be pre–registered by banks (30) and other owners, controllers, and issuers of payment systems (32). Owners of payment systems, such as corporate/purchase cards, may authorize usage by third parties within specified limits, thus enabling them to monitor and control delegated authority. A central account authority (12) provides registration services indicating which hub services which client. The VPS (10) implements a dual key transaction system, in which verified instructions must come separately and completely independently from both client (22) and vendor (24) before transaction completion via methods accepted by both parties. The VPS (10) allows the client (22), the vendor (24), and associated payment methods and systems (30–32) to be known, with fixed quantities and pre–registered within an authorization manager. The client (22) and vendor (24) may choose the payment method and currency used at each end of any transaction, and payment is always made within a closed system without either party having access to or knowing the details of the other's payment system. Real–time audit trails for all parties concerned are implemented, in which client (22), vendors (24), and banks (30) may trace transactions, generate reports, and initiate refunds for such secure transactions. The VPS (10) is also software and/or hardware independent, implemented by any known networking configuration for any known electronic or digital transaction, using mobile phones (28), palm–tops and digital television for purchases and credit/debit payment arrangements for any form of commerce using electronic transactions.



# VERIFIED PAYMENT SYSTEM

## BACKGROUND OF THE INVENTION

The present invention relates to electronic commerce and, more particularly, to a distributed payment system for implementing secure electronic commerce transactions.

## THE GLOBAL INTERNET

The Internet, in its widest sense, is becoming the global central nervous system, and is more and more often the medium for all kinds of transaction, from the personal to the multi-national. However, it is both insecure and impracticable to have to exchange primary data, such as data of diverse payment systems, each time that an electronic transaction takes place. At the same time, owners and controllers of data, including corporate, banking, and private entities, must be able to preserve their privacy and to control the mechanisms used for securely identifying themselves in order to:

access their own data;

verify their identity to each other; and

authorize transactions.

All parties to a transaction need an impartial record for the purposes of validation, automation, and reconciliation. The present invention solves these problems.

## ELECTRONIC COMMERCE

Electronic commerce is becoming more pervasive as the Internet and other communications networks are employed to facilitate consumer/vendor interactions. Beyond networks connecting banks and credit card companies to vendors for use in

In addition, known electronic commerce systems are unable to readily handle micropayments; that is, payments under a specified threshold, such as less than ten dollars or ten pounds. Micropayments are becoming more pervasive, for example, in downloading snippets of data over the Internet such as image files and icons, as well as service fees for access to on-line resources such as usage fees for accessing a website for information and/or software. In addition to such concerns as verification and authentication, there is a requirement for E-commerce to handle micropayments, and to charge the client with accrued micropayments in a single macro-settlement.

A need also exists for an E-commerce system which provides secure and authenticated micropayments.

In addition, many business transactions rely on a degree of trust and identification built up after extensive dealings. When this level of trust has not been established by a prior relationship, which is increasingly common in the competitive and mobile marketplace, a need exists for enabling a transaction by providing identification, verification, non-repudiation, and payment services to the parties of the transaction.

A need also exists for an E-commerce system which provides secure and authenticated micropayments.

In addition, E-commerce through World Wide Web (WWW) interfaces such as browsers is becoming more popular. However, such browser-based implementations are relatively insecure, for example, in requiring the use of "cookies"; that is, browser information stored on the client's Internet-accessible computer which is known to compromise the privacy and security of the client.

A need exists for an E-commerce system, including Internet-based systems,

payment is then always made within a closed system without either party having access to or knowing the details of the other's payment system. Owners of payment systems, such as corporate/purchase cards, may authorize usage by third parties within specified limits, thus enabling them to monitor and control delegated authority.

In addition, real-time audit trails for all parties concerned are implemented by the disclosed system, in which client, vendors, and banks have access to transaction records and may trace transactions and generate reports for such secure transactions. The disclosed system is also software and/or hardware independent, in that the disclosed system may be implemented by any known networking configuration for any known electronic transaction, such as using mobile phones, palm-tops and digital television implementations for purchases and credit/debit payment arrangements for any form of commerce using electronic transactions.

In addition, the system supports pre-registration of payment systems by financial institutions to improve the security of the process.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates the disclosed verified payment system;

FIG. 2 illustrates a hub of FIG. 1 in greater detail;

FIG. 3 illustrates a simplified flow diagram of operation of the verified payment system;

FIG. 4 illustrates a more detailed flow diagram of operation of the verified payment system;

14.

The network 14 may be a wide area network (WAN), a portion of the Internet, or other electronic network communications mechanisms. Each of the hubs 16-20 may also include or be operatively connected to one or more authentication systems, such as a local authentication server 34, for authenticating the electronic transaction requests registered by each client and each vendor for a given electronic transaction.

Each of the hubs 16-20 may be embodied, for example, as shown in FIG. 2, in which communications from the Internet 26 are passed through at least one firewall 36 to a secure hub-internal network 38 having a web farm 40; that is, a plurality of web servers, such as "WINDOWS NT"-based servers, for processing Internet communications such as HTML and HTTP data packets embodying, for example, electronic transactions so that the web farm 40 supports transaction requests and authentication services from other hubs 16-20. The authentication servers 34 may authenticate the payment system details associated with an electronic transaction, such as valid credit card information, and then transmit the electronic transactions data to a bank 30 or other payments systems 32 for further authorization, settlement, and processing.

The VPS 10 includes one or more databases maintained, for example, in a "WOLFPACK" SQL database server 42 which holds details on vendors 24, clients 22, and payment systems. The electronic transactions are transmitted through a router 44 and an inter-hub private WAN 14 to other hubs for communications between a client at one hub and a vendor at another hub, or vice versa, and/or for

The VPS 10 does not rely on any particular method of pre-selection of goods, which is always based on some communication directly between vendor and client.

In summary, the VPS 10 enables payment of goods and services accessed via electronic mechanisms, including the Internet, mobile/cellular phones, digital TV, etc., following the same basic procedure, without any direct communication necessary between client and vendor. Once a client has selected and agreed to pay for such goods or services, the vendor 24 identifies himself/herself to the system 10, references the transaction, and gives the transaction amount and currency. The client also identifies himself/herself to the system 10, chooses one of his/her pre-registered payment systems, and agrees to pay. The identities of both parties are verified, and the selected payment data are married together securely off-line. The transaction is authenticated in real-time via the appropriate banking or other credit gateway, and instructions are sent, if appropriate, for immediate or delayed settlement by the vendor's bank or payment agent. The vendor is updated automatically with the authentication result, and an audit trail available to all parties to the transaction is updated. Each transaction is attached to vendor and VPS reference numbers facilitating checking and refunds. A plurality of hubs provides resilience and scalability, with each hub providing authorization services to certain vendors and verification and information services on behalf of clients. A central account authority provides registration services indicating which hub services which client.

The vendor 24 requests transaction authorization from its respective hub, such as hub 16. The client 22 also requests payment authorization from the

processor 52 in step 64. The VPS 10 provides a transaction ID and a value such as a "checksum" or a secret key to the vendor 24, and the client 22 may use the transaction ID to identify the transaction, but the VPS 10 and the vendor 24 never inform the client 22 of the secret key, which the VPS 10 includes in any communications with the vendor 24. This reduces the risk of fraud on the part of the client 24.

In an exemplary embodiment, the client 22 may be using a computer 48 and accessing a website of the vendor 24 for selecting goods or services to purchase from the vendor 24, and so in step 62, the vendor 24 redirects the browser of the client 22 to verification and payment selection screens with the transaction key as a parameter of the redirect of the client 22. The interface of the vendor 24 which is provided to the clients 22 may include a website and/or other graphic user interface (GUI) environments, such as a browser using plug-ins and/or scripts to support, for example, Active Server Pages technology and/or Commerce Server Order Processing Pipeline technology associated with "INTEL" and "MICROSOFT WINDOWS", as well as Perl scripts for Unix and/or Apache environments.

Alternatively, using a telephone 50, the client 22 may select goods or services from an automated telephone service of the vendor 24, for example, using a touch-tone telephone and a series of automated audio menus. Accordingly, in step 62, the vendor 24 redirects the client to a payment selection and authorization menu through the telephone 50, or the authorization processor 52 calls back the client 22 to allow the transaction to continue.

The client 22 thus sends a request for payment authorization and/or selection

authorized client 22. If the client 22 cannot be authenticated, the vendor 24 is informed of the reasons, and so the request for transaction authorization in step 56 can be rejected. Otherwise, the vendor 24 may perform a fulfillment transaction or a normal transaction to complete the authorized transaction for an authenticated client 22. Other conditions such as refunds may also be handled.

FIG. 7 illustrates the processing in FIG. 5 in the Waiting for Client Details state by the authorization processor 52 in step 66 of FIG. 4 to check and authenticate a purported client, in which the authorization processor 52 waits to receive registration information from the purported client. Each authorized client has registered previously, so the authorization processor, upon receiving the client details, attempts to match the purported client with one of the authorized clients, and upon a match, obtains the client details 68.

FIG. 8 illustrates the processing in FIG. 5 in the Attempt Authorization state performed by the authorization processor 52 in steps 64, 66, and 70 of FIG. 4 to authorize a request for payment from the client 22 of FIG. 4 to present payment choices to the client 22, and to process the payment selection, which may be a Normal payment system, that is, a full amount of the transaction is applied to the payment system associated with the client; or which may be a Micropay payment system, that is, transaction charges less than a predetermined amount are accrued and applied latter to the client 22 after the accrued amount exceeds a predetermined threshold, or to reduce an outstanding float which is topped up when the float reaches, for example, zero.

In the case where the client details 68 are stored in a different hub from the

independent supplier of the VPS 10. A financial settlement service is defined as an institution responsible for the actual transfer of funds, such as an acquiring bank for credit cards, but may include other financial institutions.

Typically, the payment system owner is the individual holder of a credit card, but a payment system owner may also be an officer of a company holding a corporate credit card or purchase card, or, indeed, the accounts head who controls a billing account payment system. As described herein, an autopay feature is defined as a feature allowing a client to enter a uniquely assigned user name and/or a personal identification number (PIN) only once during a session rather than entering such data for each purchase. The payment system owner may be any individual holder of a payment method, such as a credit card owned by a client, with the holder being a company officer responsible for the payment method, such as an officer, an accounts head, and/or a procurement official of a company holding, for example, a corporate credit card and/or other billing accounts associated with use by the payment method.

Using the disclosed VPS 10, clients 22 are able to make payments to VPS vendors 24 via the Internet 26 or other communications networks. The information and details about each client 22 associated with a credit card or other payment system 32 are never transmitted clear across the Internet 26 or other communication network, but instead are only transmitted in encrypted form to allow a client 22 to add or amend his/her account. Alternatively, Internet-based account modification may be avoided by allowing the client 22 to provide credit card details or other payment system details by facsimile or other secure data transmission mechanisms.

payments by providing an automatic conversion to a common currency in the authorization processor.

Optionally, an Autopay feature may be implemented in which, with the client's explicit agreement, the identification process can be set to be transparent after a initial identification during a session involving a client with a specific vendor. Such transparent transaction processing provides a simpler process for a sequence of transactions, while maintaining comparable security.

Access and use of a given payment system 32, such as a credit card system, may be granted by the owner of the payment system to other VPS clients 22. The owner specifies credit restrictions for the authorized client and is able to view all transactions. The authorized client is only able to see transactions which that client has instigated.

Clients 22 may be "pre-loaded" by financial settlement services, vendors or companies, such that the pre-loading process creates a set of inactive accounts which the designated client can activate through the use of a personal identification number (PIN) sent separately by the client. Pre-loaded accounts may be subsumed into an existing VPS account by the client, or may be used to create a new account.

Vendors 24 may issue refunds through the VPS 10, and clients 22 and vendors 24 may authorize payments to other clients, such that the VPS 10 provides flexibility and adaptability to different marketing and sales methods.

Vendors 24 may choose to provide account facilities to specific clients or groups of clients. These account systems may seek payment through a financial settlement service when the account exceeds a certain limit, in a form of Micropay,

and password on a secure web connection. Alternatively, any other form of identification and verification may be used, including smart cards, digital certificates and signatures, and/or biophysical/biometric-based identification methods. The payment systems 32 and/or the client data may be hosted by other organizations external to the VPS 10.

## FEATURES OF THE VERIFIED PAYMENT SYSTEM

The VPS 10 is a value-added authentication and settlement system which is convenient to use and offers unprecedented levels of security. The VPS is a trusted third party system holding details of payment systems belonging to buyers, sellers and providers of credit, in a secure environment, to provide the link between the parties involved in electronic fund transfer or credit account transactions, such as banks and other providers of credit, buyers and sellers. The VPS 10 permits these parties to authorize transactions and/or to exchange funds rapidly and efficiently, without disclosure or exposure to risk of sensitive data, and to automate their processes. Also, the VPS 10 provides an impartial, real-time audit trail to all parties - clients, vendors, banks, etc. - of all transactions for which the VPS 10 is the enabling service.

When a client first opens a VPS account on the Internet, the client enters credit card or other payment system details, including bank and credit accounts, through a secure interface to the VPS 10, such as a secure website or other secure data entry mechanisms. The relevant information is passed securely and protected, for example, by SSL encryption via a web server of the VPS 10, or other secure

step 74, so that client and merchant can be quickly informed of the result within, for example, within three to seven seconds.

Each transaction is uniquely identifiable via codes assigned by the merchant and by the VPS 10, thus facilitating reference checks, monetary credits, and refunds. An autopay feature allows the client 22 to identify himself/herself only once for all transactions within a single session with a vendor 24, for example, on the respective vendor's website.

Very small payments may be specially processed, in which all payments below a minimum predetermined amount agreed to by each merchant are classed as micropayments and treated separately. Micropayments are part of a seamless service offered to merchants and account holders who use the VPS 10, by which such micropayments accrue and are totaled up until the account holder makes a transaction which causes the accrued sum owing above the threshold of the minimum amount. The VPS 10 then automatically seeks payment for the total of outstanding micropayments plus the new transaction. Merchants using the VPS 10 may thus choose from two payment options. Using the first option, merchants using the VPS 10 may choose to receive payment directly and to allow their clients to purchase goods and services on credit without pre-payment up to an agreed threshold. No payment is debited to the client until the threshold set by that merchant is reached, and the merchant then receives payment for all micro payment transactions as one consolidated sum. This allows the clients to purchase small goods and services incrementally, such as downloading small files of information or programs such as applets, as well as data such as search engine queries.

systems as desired in one virtual wallet, such as payment systems including business and personal accounts paid monthly in arrears, accounts paid by direct debit etc. Such registered payment systems of an account holder are accessed via identity checks, and such card and other payment system details may be pre-registered by the issuer, so that card holders never have to put their card or personal details on-line. Such off-line information gathering and retention ensures that addresses are true billing addresses, and so the VPS 10 is enabled to run accurate address checks on behalf of merchants without divulging any account holder information to the merchants.

In accordance with the standard initial operation of the VPS 10, the account holder chooses a unique combination of user name and alpha-numerical password as a PIN, and logs additional security information into the VPS 10 to be used as an identity check at any time thereafter. Random questions based on the additional security information are mandatory for all changes to a client's account, and such questions are optional for transactions and consultation of audit trails. PINs and additional security inputted by an account holder may be always disguised as asterisks or blank spaces onscreen. A prompt mechanism may be provided to help people with short memories. Other forms of identification and verification can be accommodated as deemed appropriate by banks, financial systems, and major users. The account holder also may choose spending limits to self-limit expenditure.

On-line audit trails having, for example, a resolution for time intervals down to the second, including for micropayments, are provided for users and vendors. Accounts can be controlled on-line by the user, so that details of purchases can be

authority 12 detect six errors in different transactions in one period of twenty-four hours, the account may also frozen.

The VPS 10 initially uses a combination of user name, password and security checks, as in known telephone-based banking, to identify account holders, such as the use of random questions based on two words and one date. However, the VPS 10 may also be configured to accept other forms of identification and verification, such as digital certificates and signatures, voice recognition, iris recognition, thumb print recognition, and other known methods for authenticating a user accessing the VPS 10 as a purported authorized user. For example, identification via smartcards may be included in the authorization processor 52, and so the VPS 10 can therefore work well with smart card-based systems, providing direct links into account holder credit/debit card accounts, micro payments without pre-payments, online audit trails, etc.

For merchants and vendors, the VPS 10 provides all participating merchants with a safe and cost-effective method for collecting payments. Payment may be made directly to merchants via their own banks and merchant numbers. The VPS 10 is designed to enable merchants to build client loyalty and brand recognition by, for example, assuring clients of security and privacy by both client and merchant participating in the VPS 10. Since the VPS 10 supports credit as well as debit operations, the VPS 10 also facilitates cash-based client incentive schemes and diverse kinds of loyalty-generating promotions conducted by the merchants. The VPS 10 may also provide a particular merchant with marketing and client intelligence about the merchant's own clients, sales patterns, and global report,

notification being integrated as part of the merchant's transaction sequence, thus allowing automation and control over the security of the validation process. Full integration with existing systems owned by the merchants and vendors also enables seamless integration with ordering, accounting and other software products.

To participate in the VPS 10 as acceptors of payment by credit or debit card, merchants using credit cards obtain E-commerce-enabled merchant numbers from their acquiring banks. The VPS 10 may allocate Terminal ID (TID) numbers to merchants from the range set aside for each bank, and then the VPS 10 informs the bank so that settlement can be made directly to the merchant.

The VPS 10 uses a distributed hub arrangement in order to provide full scalability and optimum performance as a universal and global system. Regional hubs 16-20, either single or clustered, guarantee fast reliable worldwide access and redundancy. Hubs are either operated directly by the VPS 10 or as a series of inter-locking joint ventures between the VPS 10 and a hub operator, such as a bank, a group of banks or other clearing houses or financial institutions. Merchants and account holders have one "home hub", as shown in FIG. 1, but VPS accounts may be used worldwide. Standard transactions are authenticated and settled via links between the merchant's hub and the merchant's corresponding bank, while micro-payment transactions may be processed via the account holder's hub.

Safe international direct debits are performed, such that the global banking system can be used to send sums from an account in a bank in one currency zone to an account in a bank in another currency zone. Businesses, merchants, and vendors may acquire funds; that is, receive payment into designated bank accounts, in at

abuse them, since the payment systems can only be used to transfer sums to merchant number accounts held by vendors within the VPS 10.

Credit card systems and other payment systems used exclusively for the transfer of funds from one source to another can be registered within the VPS 10 and locked to this exclusive use, thus providing an entirely secure closed circuit. Although the VPS 10 may operate via the Internet 26, the VPS 10 is not dependent upon the Internet 26, as all key processes performed by the VPS 10 occur off-line. Major clients, managing large fund flows, may choose to communicate with the VPS 10 via dedicated leased lines. In the case of direct debits and closed circuit usage, no sensitive information is ever exchanged via the Internet 26, thus avoiding the need for high level encryption, digital certificates etc. to be used by the VPS 10, which increases the complexity and cost of use of the VPS 10. Accordingly, the VPS 10 provides an extremely simple and safe method to transfer inter-currency commercial sums.

The VPS 10 also provides a universal and globally-expandable system for E-commerce, being a truly distributed system in which one ID allows users and vendors to mediate all transactions via the same globally accessible system, with the hub design provides quick service and back-up facilities. In addition, pre-registered credit cards may be used, so that new on-line registrations and address and personal information checks for each client for each credit card are not necessary. Furthermore, card issuers may open dormant VPS accounts on behalf of their card holders by registering card details plus names and address, as well as temporary PINs and a temporary user names for each account, which may also be generated for

implemented, so that a father can authorize his children to use his credit card up to a fixed amount; a company can authorize a department or individual to use a corporate purchase card within a budget and within purchasing parameters, for example, the use of the account can be tied to specific goods, services, and/or vendors and clients. A supplier can authorize a client company to use a credit account, which can in turn be subdivided among departments and individuals. The account holder can monitor and control all transactions using his/her payment system via an on-line VPS audit trail. Users are never given the details of the payment system, such as the card numbers used, or given VPS ID used by the account holder. Clients may have registered payment systems which they do not own but have permission to use and associated with their VPS virtual wallets with their other payment systems. Using VPS virtual wallets, clients may pay for goods and services and to monitor spending, via their own VPS ID. This very flexible system is also the basis for setting up store card accounts and direct debits, including payment of utilities and monthly credit accounts. In this case, the account holder gives the vendor permission to use his payment system, such as a credit card account, to take regular payment for agreed goods and services.

## OPERATION OF THE VERIFIED PAYMENT SYSTEM

Typically, the VPS 10 uses the following principal data for each client: name; address and contact details; E-mail address; security information such as user name, PIN, security prompts and authorization PIN for bulk loaded accounts; confirmation code such as a code by which a client informs potential fund

To manage client accounts, the account administrator may add a new account, disable or enable an account, delete an existing accounting, change and/or view personal, security, and/or payment system details of the client associated with the account, and change and/or view client preferences.

The pre-loading of accounts is a customizable operation, since the data format for account information may be different for each payment system. The accounts may be pre-loaded into a holding table, and the corresponding account owner is notified of the holding table and the status of the pre-loading, for example, by a hardcopy letter to the owner. This notification may include an access code, so that the account owner can access the VPS 10 and use the access code to create a new account using a selected payment system 32, or add a new payment system to the owner's existing VPS account.

As to the vendors 24, the VPS 10 may retain the following principal data about each vendor: name; address; security user name; security PIN; authorizing payment system; bank information such as TID, sort code, and account number for payments; account, client, and transaction details for vendor-specific micropay or billing accounts; security/payment preferences; commission details; contacts; Internet Protocol (IP) Domain; and category of business. Each of the vendors is operatively connected to at least one of the hubs 16-20, which supports the vendor and manages all the transactions with the vendor and transaction-initiating clients. To be set-up, a vendor completes an agreement and provides bank authorization to the VPS 10 for third party TID payments and for a payment system, such as direct payments, or debit or credit cards, which allow fees to be extracted. These payment

include a type of micropayment facility in which the client's payment system is only debited when a certain total value of transactions are reached. Thus the client may have purchased, for example, four or five items over a couple of weeks before his/her card is debited, and/or when the total reaches, for example, U.S. $20. A second form is a "normal" billing account between the vendor and potentially a large client, in which the VPS 10 mediates the transactions and provides billing information to the vendor, but the vendor invoices the client directly. The vendor sets a credit limit on the billing account, and such a payment system may be considered to be owned by the vendor and granted to clients, for example, through the agency of authorized clients.

The vendor may choose to pay money to a client, for example, as a reward for loyalty, as a refund, or as a payment of winnings or promotional activities of the vendor. The payment may be on the back of a transaction made earlier, so that the vendor does not need to know the clients details, as enforced by the VPS 10. A transaction code from the vendor is used to identify the client, the credit card or payment system information, and the refund as being performed appropriately. If the credit card is no longer valid, the money equivalent is transferred to an holding account and the client may be notified, for example, via E-mail. The client may then use an interface associated with the vendor and/or with the VPS 10 to specify which payment system is to be credited.

If the client of the credit card or other specified payment system is no longer on the account authority 12 of the VPS 10, the vendor is notified, and the VPS 10 undertakes to mail, send via facsimile, or send via E-mail a notification to the client

client, such as U.S. $ 500 on one credit card and U.S. $ 400 on another credit card to overall charge U.S. $ 900 for the single transaction.

If the client has a preferred payment system, then the preferred payment system is chosen automatically unless the transaction is Micropay and the preferred payment system does not support Micropay, or the preferred payment system is not supported by the vendor. Normally, the user selects which payment system to be used from a list of available payment systems which are compatible with payment systems supported by a particular vendor.

After either success or failure of a transaction, the client is returned to an appropriate point such as the website where the client was present before initiating the transaction.

Autopay is a feature which may also be supported by the VPS 10. Autopay is a process by which a client merely confirms his/her personal VPS ID once in a session of transaction. After the first payment in a session, a series of data transfers, which may optionally include browser-oriented cookies for Internet-based E-commerce, is used to confirm the identity of the client. Such cookies do not include secure information, are deleted on entry into a new session, and have a limited lifetime. Autopay may also time-out if there are too large gaps in time between individual transactions.

The VPS 10 may also generate many different reports for different purposes, as described in Table 1. In general, report and statements include dates, vendor and transaction codes, and the sums involved. Such reports only include methods that allow the client to be identified if both a vendor and a client agree to such client

that the client's user details have been stolen.

Intra-hub security is implemented in a number of levels. At the top level, a supervisor controls the access rights of operators but may not themselves have rights beyond this management function. At least two passwords may be held by different individuals, and lodged with trusted third parties to cover emergency conditions. Details of encryption methods are to be known to the chief technology officer (CTO) of the VPS 10, as well as to any necessary delegates. Such details may be securely lodged externally. All source code supporting security is also password protected. The purpose of this top level of security is to access and manage the inherent security of the VPS 10. In general, users at this top level are restricted to limited areas of the VPS 10.

The second level of security allows management of internal users of the VPS 10. The users at this level and their properties and access privileges can only be changed by top level security people, but the second level users have the ability to grant access to operators of the VPS 10. In addition, these second level users are able to examine and/or generate audit trails as required. The audit trail for an acquiring bank may include all of the credit card details of a client.

The third level of security includes normal users and staff of the VPS 10 who have access to client and vendor accounts, typically to amend details, enter credit card information received by fax, and confirm transactions to clients and vendors with appropriate identification. All sensitive data, such as payment system details, are held in the database 42 encrypted to a high level of security.

Inter-hub security is provided such that all communications between the

rejections to a vendor may also be identified in the event of system failure.

For such operational performance, the Microsoft Message Queuing (MSMQ) system may be used for communications between the hubs 16-20, which may guarantee the state of all communications. Typically, in one embodiment, around 8 transactions per second per node can be supported on a single ISDN channel, up to 128 transaction per second (tps) on a 1 MB link, which is about 11 million transactions per day. At this rate, the costs of a 1 MB pipe are insignificant compared to the benefits in providing such high speed transaction processing.

MESSAGE FORMATS

A preferred embodiment of the VPS 10 uses the HTTP "POST" protocol to dispatch service requests, to receive service results, and to permit interaction with vendors and clients. Other embodiments would include message queuing services, DCOM, and so on. The formats of a number of example messages and responses for interfacing with components of the VPS 10 are described herein which form the kernel of the operational side of the VPS 10. In an Internet-based embodiment, post data is Universal Resource Locator (URL) encoded, and may be sent as if the post data were dispatched by a SUBMIT button or icon on a form of a GUI. The AuthorizeTransaction message may be purely intra-hub, while other messages such as CheckLimitsAndGetPSDetails, CheckLimitsAndAuthorizeMicropay, BulkNotification, and TransactionAbandoned may be inter-hub, or may be intra-hub if a client and vendor are on the same hub.

The AuthorizeTransaction message is a packet which is dispatched an authentication server queue, in which a request packet is sent as follows:

either returns an error or the payment system info. The request packet for the CheckLimitsAndGetPsDetails post includes:

| Name | Type | Description |
|---|---|---|
| Size | Short | Size of the packet (including this word) |
| Version | Short | Version of packet format. This allows for more transparent upgrades of software |
| TxType | short | Payment, refund, micropay .... |
| VendorHub | Short | Hub Where Vendor is |
| Vendor | Long | Identifies Vendor. Only needed for Tx Log. |
| ClientHub | Short | Hub where the client lives |
| ClientID | Long | ID of client |
| OurTxCode | GUID | |
| VendorTxCode | Char[20] | Vendors transaction code |
| TransactionStartTime | Datetime | When the transaction started |
| PaymentSystem | Long | Payment System which the Vendor will attempt authorization on |
| PreviousPS | long | Previous payment system if a repeat attempt |
| Amount | Money | How much for |
| Currency | Char[3] | Currency of request |
| OriginalAmount | Money | What the request was for in original currency (mainly micropay) |
| OriginalCurrency | Char[3] | Original currency |
| Return IP | IP | Represents originating machine. This will principally be used when we move to asynchronous processing |
| AddressNo | Long | Address Identification |
| Index | Short | Indicates if this is the first attempt at authorization or greater. |

The corresponding response packet is:

| Name | Type | Description |
|---|---|---|
| Size | Short | Size of the packet (including this word) |
| Version | short | Version of packet format. This allows more transparent upgrades of software |
| OurTxCode | GUID | |
| ResponseCode | short | ExceedsLimit(type), invalid system, invalid client, has PS details, has address |
| PaymentSystemDetails | Varchar[100] | May be empty |

| | | |
|---|---|---|
| | | have it's own number if appropriate (and a different hub), but can be reconciled in the OurAuthCodes table |

The BulkNotification post or put includes any number of batched notifications which indicate that a transaction has been settled, a deferred fulfillment has been cancelled, or the settled transaction has been charged back and post-settlement cancellation is performed. The packet thus has a header indicating version, total size and number of entries in each of the three sections, followed by three sections with details on the items mentioned above. The request packet is:

| Name | Type | Description |
|---|---|---|
| Size | Short | Size of the packet (including this word) |
| Version | short | Version of packet format. This allows more transparent upgrades of software |
| SourceHub | Long | The hub the message comes from |
| NoSettledTransactions | Long | Number of entries in the 'settled transactions' section |
| NoCancelledDeferred | long | Number of deferred fulfillment Txs which have been cancelled |
| NoChargeBacks | Long | Number of 'bad' settled transactions |
| DATA | DATA | Block of data corresponding to the volumes of settled, cancelled and charged back respectively. |

The Settled TX format is:

| Name | Type | Description |
|---|---|---|
| OurTxId | GUID | Transaction that was settled |
| SettlementBatch | long | BatchNumber of the settlement |
| SettlementTime | Datetime | When it was settled |

The Deferred FulfilmentCancellation format is:

| Name | Type | Description |
|---|---|---|
| OurTxId | GUID | Transaction that was cancelled |
| CancellationTime | Datetime | When it was cancelled |

The Charge Back format is:

IP=255.255.200.2

XML formatted messages may also be used. Encryption of the contents of the message may also be performed.

The Vendor Transaction Start message is sent by the vendor to indicate that the client wishes to make a purchase. The VPS 10 registers a transaction in a transaction table and returns the transaction code and IP address for future client communication. The parameters may be:

| Name | Purpose | Constraints |
|---|---|---|
| MESSAGE | Indicates type of Message | "PAYMENT" |
| VendorTxCode | This identifies the Transaction to the Vendor | 20 character max length. Unique for a given Vendor |
| Description | Free text summary of the products bought | 64 characters. |
| Amount | Total Value of Transaction | Numeric string. |
| Currency | Currency of Transaction | As used in APACS (GBP, USD ...). Must be a 'supported' currency that may be vendor specific. |
| Deferred | Indicates that settlement is not to be sought until the vendor requests it (normally due to goods not being in stock) | "Y" or "N". Default is "N" if form variable not present |
| Micropay | Indicates that a Micropayment Method is required (vendor or client) | "Y" or "N". Default is "N" if form variable not present. Transactions below a certain Payment System Type defined level will ONLY be accepted as |

| | | |
|---|---|---|
| | (No Amount, for example). A free format string describing the error. | 100 chars |

A Vendor Fulfillment Notification message is sent when the vendor wishes to fulfil a deferred fulfillment transaction. The parameters are:

| Name | Purpose | Constraints |
|---|---|---|
| MESSAGE | Indicates type of Message | "FULFILL TRANSACTION" |
| ICE_TX | Which transaction is to be fulfilled | 20 chars (probably a GUID) |
| Post_Notify | In some cases we can simply return a code that indicates the state of the transaction (done, dropped). In others, however we must re-seek authorization. By default we will provide an immediate return code where possible. However, it may be simpler for the Vendor to only process asynchronous responses. | "Y", "N". default is "N" |
| Notification_URL | A URL to return future notifications to (for this transaction and while active). Allows the Vendor more control over the organization of their site | IP |

The message returns:

| Name | Purpose | Constraints |
|---|---|---|
| RESULT | The return code indicates that the transaction is accepted, has expired, is not known or will take a little time to process. In this latter case a Transaction Complete Notification will be sent. | "ACCEPT", "EXPIRED", "UNKNOWN", "AUTHORIZING" |

A Vendor Credit against Transaction message is sent to instigate a credit against a transaction. The credit may be simply for the purpose of refund or may be intended to pay winnings etc. The parameter are:

| Name | Purpose | Constraints |
|---|---|---|
| ICE_TX | Identifies the transaction to the VPS 10 | 32 character max length. |

The message has no specific return, which depends on the processing which occurs to respond to the request.

The Transaction Complete message is sent to the vendor website, which is specific by either a default URL or the one specified in the initial Transaction Request message, when an active transaction completes normally. The parameters are:

| Name | Purpose | Constraints |
|---|---|---|
| MESSAGE | Indicates type of Message | "TRANSACTION COMPLETE", "FULFILLMENT COMPLETE", "CREDIT COMPLETE" |
| VendorTxCode | This identifies the Transaction to the Vendor. If the transaction is a deferred fulfillment or a credit against a transaction, this will be the original ICE Tx code. | 20 character max length. |
| ICE_TX | Our transaction code | 20 chars |
| VPS_CHECK | A "secret" which must match the original "secret" sent to the vendor | |
| Status | The result of the transaction. The status indicates authorization, rejection, client abort or system failure | "ACCEPT", "REJECT", "ABORT", "FAIL" |
| Timestamp | Time at which Transaction was accepted, rejected etc. | Date Time (?) |

The message returns

| Name | Purpose | Constraints |
|---|---|---|
| RESULT | Indicates that the Vendor has received the notification. In the case of a "SYSTEM ERROR", the transaction must be backed out. | "OK", "SYSTEM ERROR" |
| Timestamp | Date time when the Vendor completed | Date Time |

implemented by any known networking configuration for any known electronic transaction, such as using mobile phones, palm-tops and digital television implementations for purchases and credit/debit payment arrangements for any form of commerce using electronic transactions. In addition, the uniform currency used by the VPS 10 may be the British pound sterling, the Euro, the Eurodollar, or any other predetermined currency or monetary/financial denomination. Accordingly, the invention has been described by way of illustration rather than limitation.

3. The VPS (10) of claim 1, wherein the hubs (16-20) store client and vendor data, including user names, digital certificates, and payments system data, and wherein the hubs (16-20) prevent private data from being conveyed to the parties of a respective electronic/digital transaction during processing and completion of the electronic/digital transaction as a secured electronic/digital transaction.

4. The VPS (10) of claim 2, wherein each of the plurality of hubs (16-20) includes a respective authorization processor capable of authorizing and/or verifying electronic/digital transactions and/or initiating a payment through a financial institution.

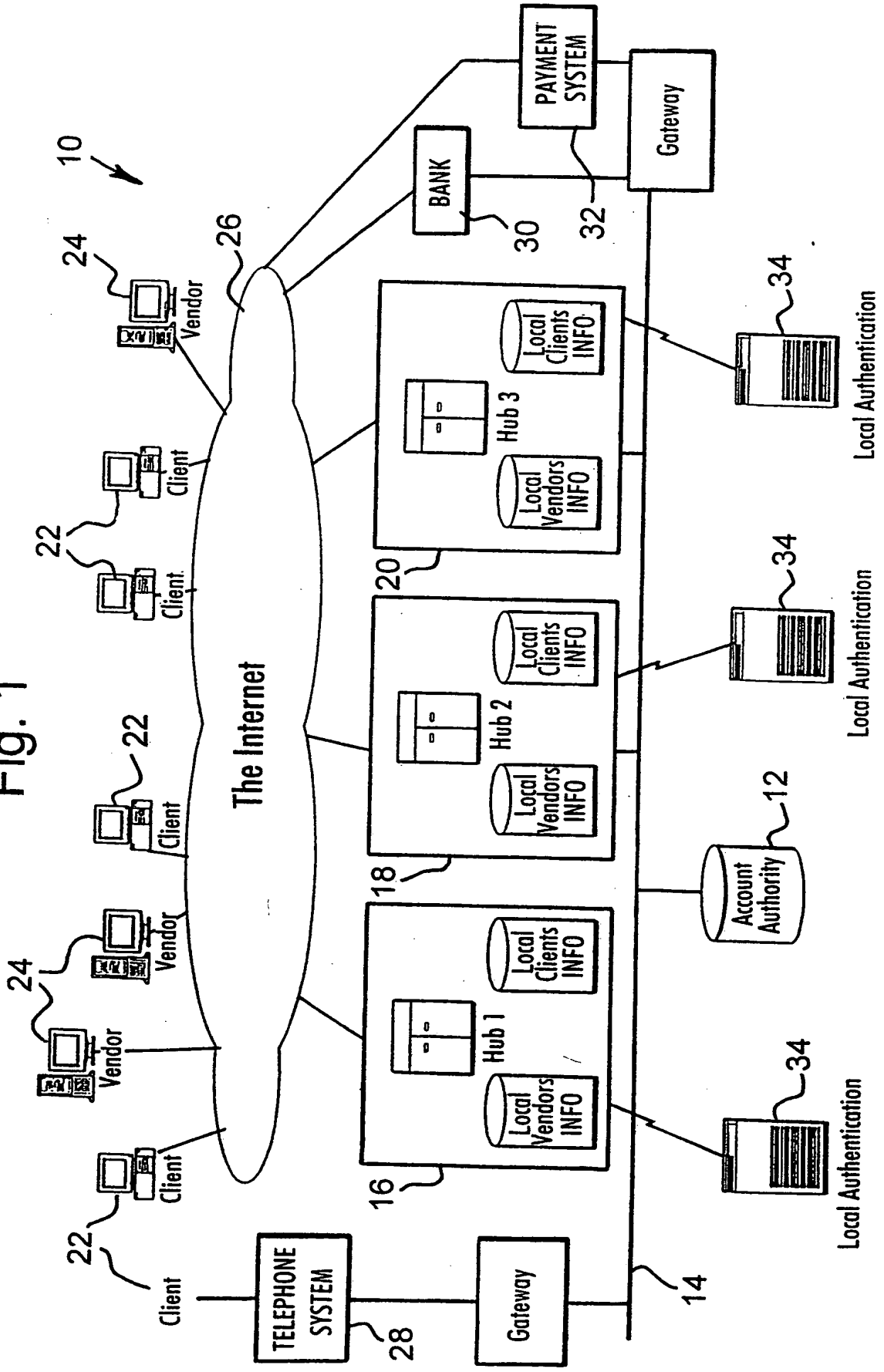
5. The VPS (10) of claim 1, wherein a set of rights-to-use a respective payment system, including a credit card system, are granted by an owner of the respective payment system to clients of the VPS (10).

6. The VPS (10) of claim 1, wherein the vendor (24), responsive to authorization of the electronic/digital transaction, directs the client (22) to the authorization processor (12).

7. The VPS (10) of claim 6, wherein the client (22) and the vendor (24) are connected to the plurality of hubs (16-20) through at least one network (26) to initiate and enable the electronic/digital transaction.

8. The VPS (10) of claim 7, wherein the network (26) is one or more

Fig. 1


10
The Internet
26
Vendor
24
Client
22
BANK
30
PAYMENT SYSTEM
32
Gateway
Hub 3
Local Clients INFO
Local Vendors INFO
20
Hub 2
18
Hub 1
16
34
Local Authentication
Account Authority
12
TELEPHONE SYSTEM
28
14

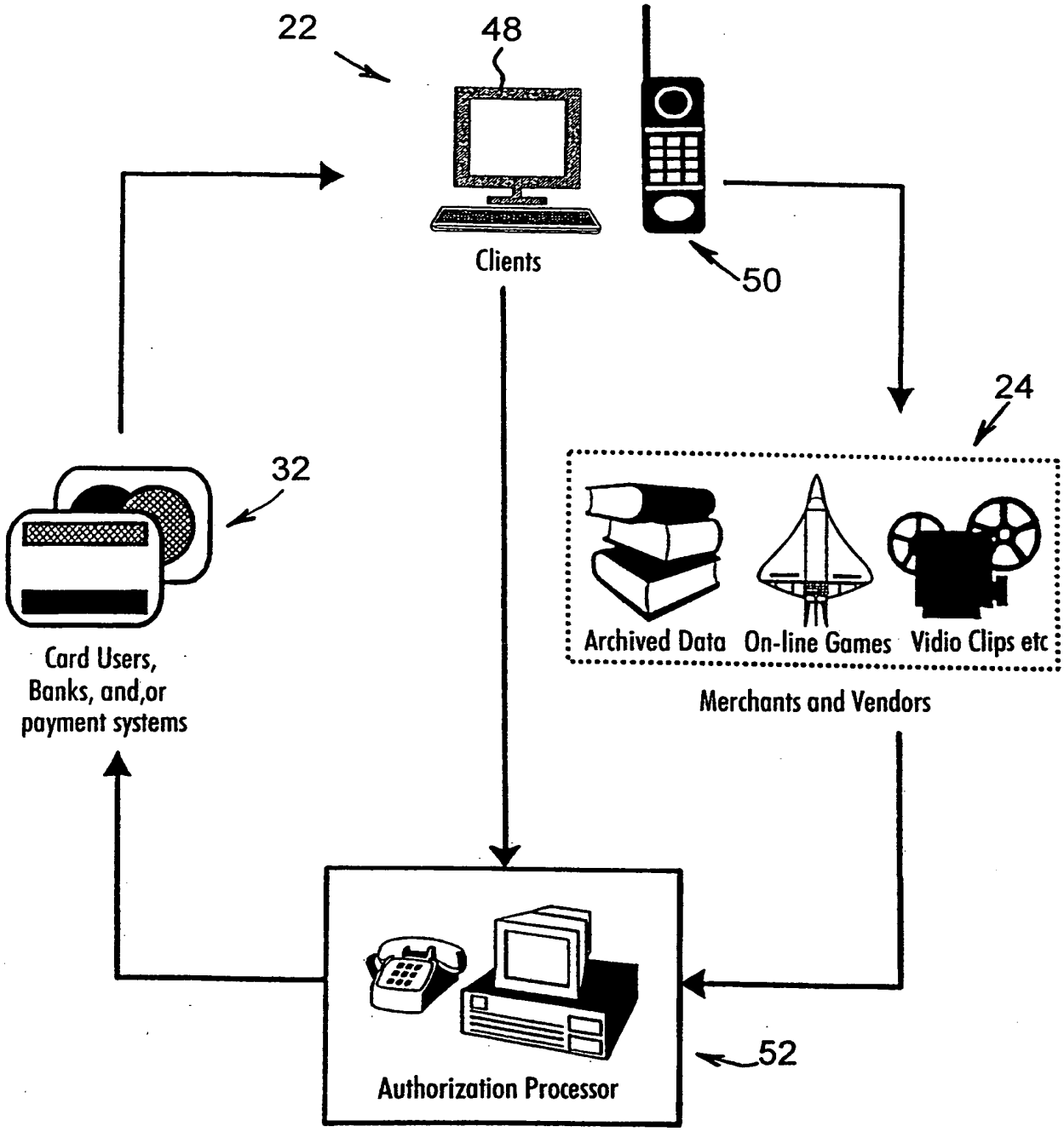

22
48
Clients
50
24
32
Archived Data
On-line Games
Vidio Clips etc
Merchants and Vendors
Card Users,
Banks, and,or
payment systems
52
Authorization Processor

Fig. 3

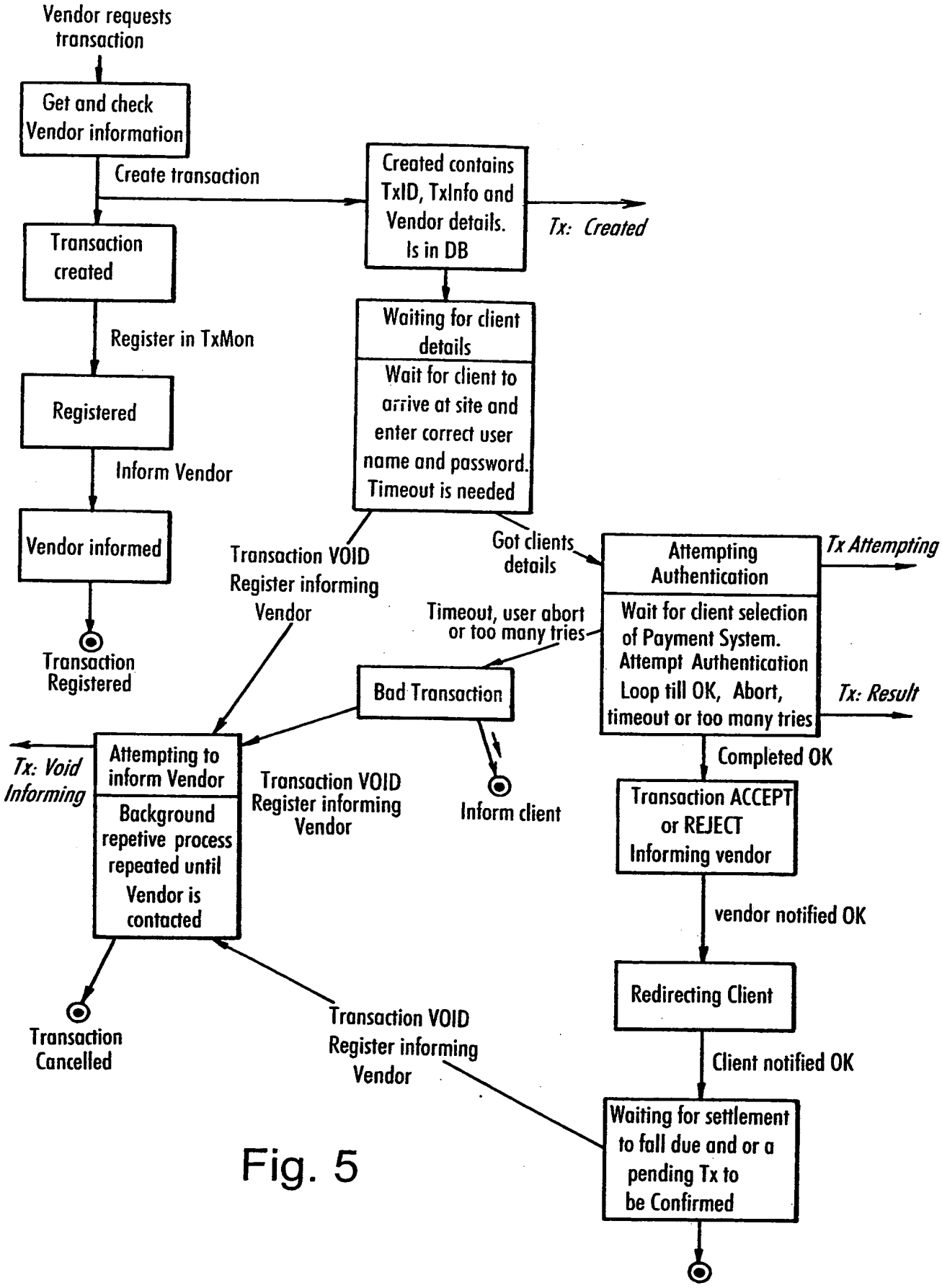

Vendor requests transaction
Get and check Vendor information
Create transaction
Created contains TxID, TxInfo and Vendor details. Is in DB
Tx: Created
Transaction created
Register in TxMon
Registered
Inform Vendor
Vendor informed
Transaction Registered
Waiting for client details
Wait for client to arrive at site and enter correct user name and password. Timeout is needed
Transaction VOID Register informing Vendor
Got clients details
Attempting Authentication
Tx Attempting
Timeout, user abort or too many tries
Wait for client selection of Payment System. Attempt Authentication Loop till OK, Abort, timeout or too many tries
Tx: Result
Bad Transaction
Completed OK
Tx: Void Informing
Attempting to inform Vendor
Background repetive process repeated until Vendor is contacted
Transaction VOID Register informing Vendor
Inform client
Transaction ACCEPT or REJECT Informing vendor
vendor notified OK
Redirecting Client
Client notified OK
Transaction Cancelled
Transaction VOID Register informing Vendor
Waiting for settlement to fall due and or a pending Tx to be Confirmed

Fig. 5

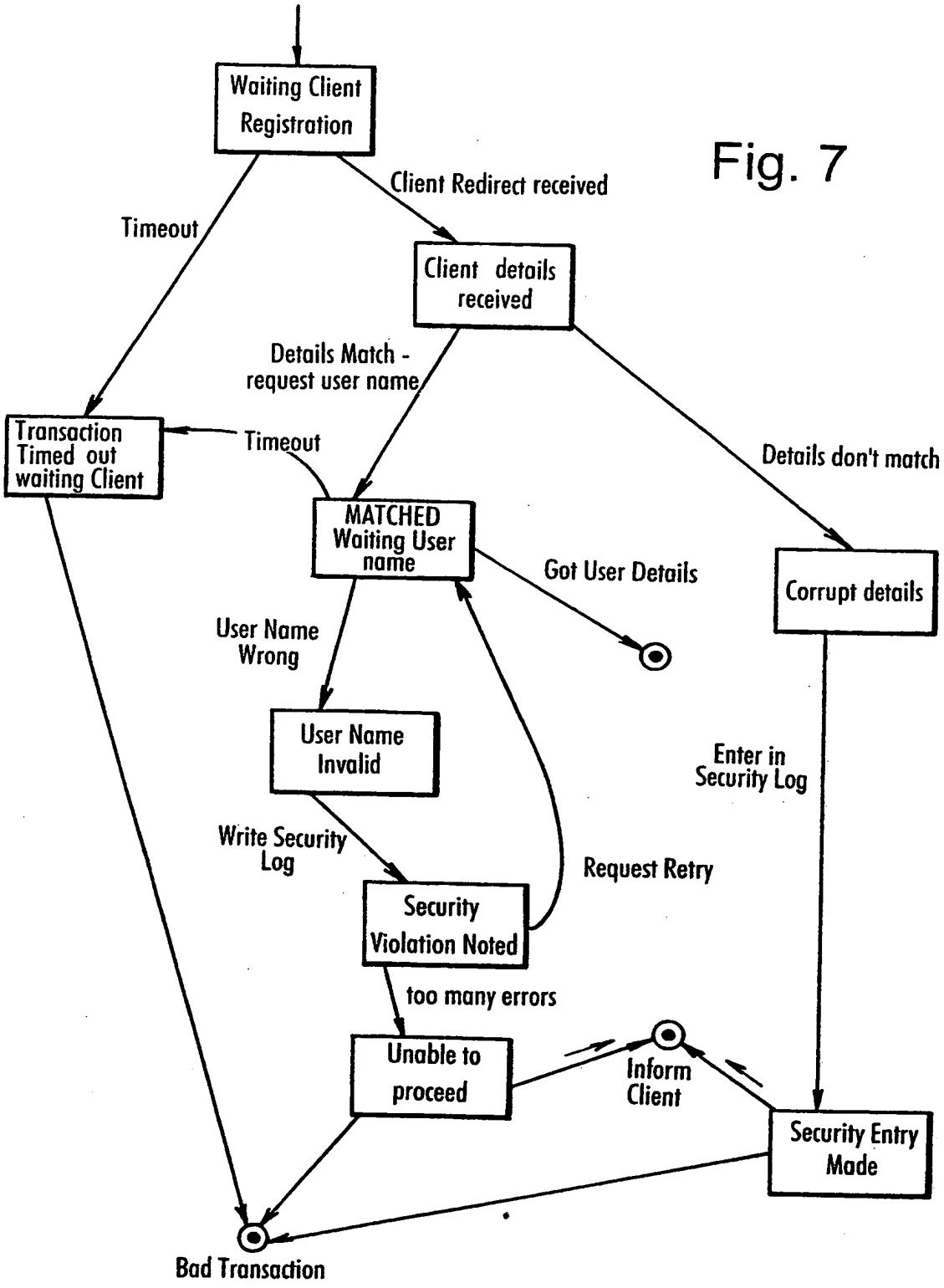

Waiting Client Registration
Client Redirect received
Timeout
Client details received
Details Match - request user name
Transaction Timed out waiting Client
Timeout
Details don't match
MATCHED Waiting User name
Got User Details
Corrupt details
User Name Wrong
User Name Invalid
Enter in Security Log
Write Security Log
Request Retry
Security Violation Noted
too many errors
Unable to proceed
Inform Client
Security Entry Made
Bad Transaction

Fig. 7

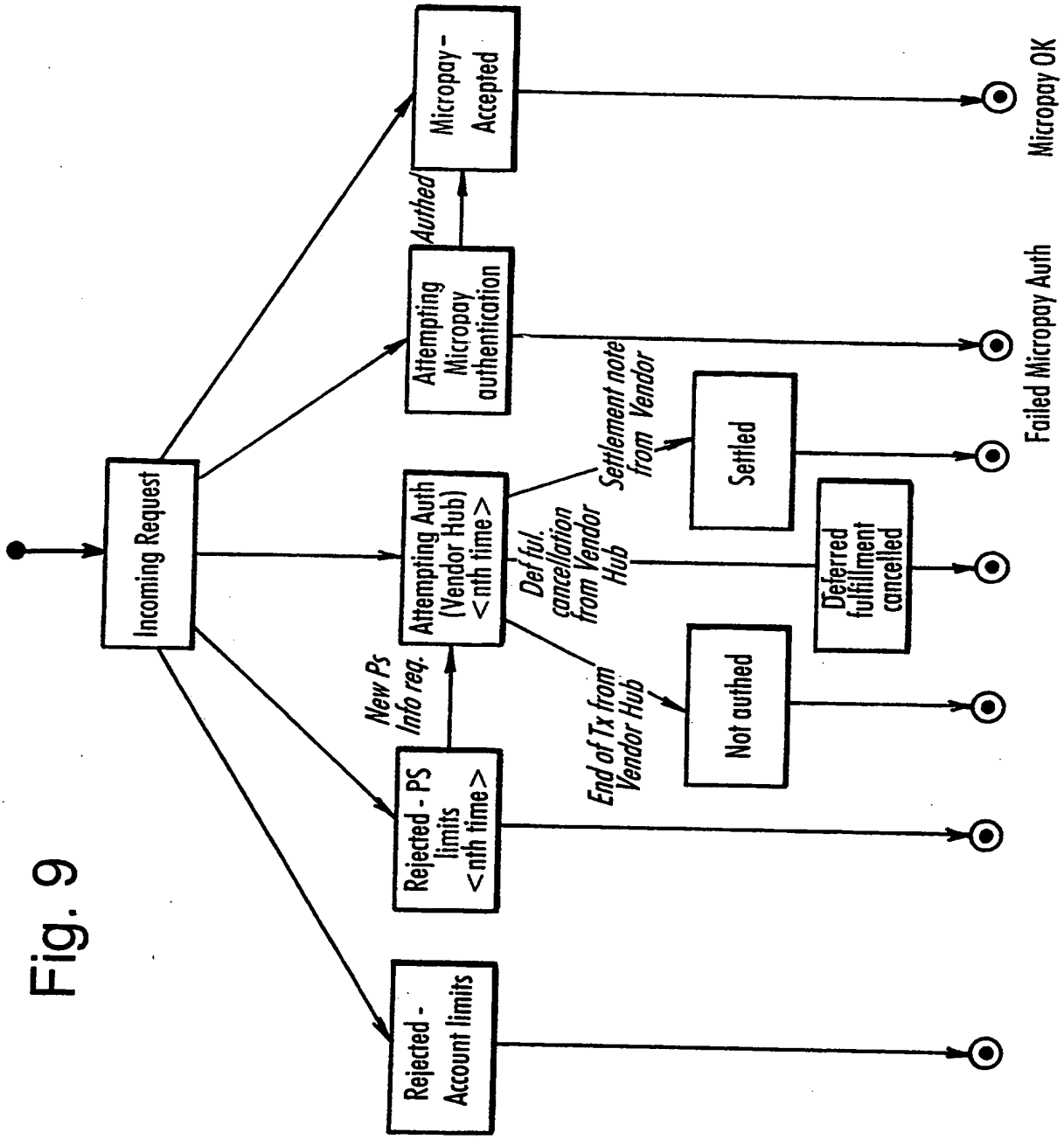

Incoming Request
Micropay - Accepted
Micropay OK
Attempting Micropay authentication
Authed
Failed Micropay Auth
Attempting Auth (Vendor Hub) < nth time >
Settlement note from Vendor
Settled
Def ful. cancellation from Vendor Hub
Deferred fulfillment cancelled
New Ps Info req.
End of Tx from Vendor Hub
Not authed
Rejected - PS limits < nth time >
Rejected - Account limits

Fig. 9

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category · | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | TYGAR: "Atomicity in Electronic Commerce" PROCEEDINGS OF THE FIFTEENTH ANNUAL ACM SYMPOSIUM ON PRINCIPLES OF DISTRIBUTED COMPUTING, 23 - 26 May 1996, pages 8-26, XP000681001 Philadelphia, PA, US the whole document --- | 1-10 |
| A | BRANDS: "Electronic Cash on the Internet" PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY, 16 October 1994 (1994-10-16), pages 1-21, XP002021041 San Diego, CA, US the whole document --- | 1-10 |
| P,A | WO 98 40809 A (CHA TECHNOLOGIES, INC.) 17 September 1998 (1998-09-17) the whole document ----- | 1-10 |